**Home Lab:**

**Project Network Security, Ethical Hacking:**

* Conducting a Vulnerability Assessment for New Web Application:

**Question 1**

1.1)

First, I installed the virtual software which is called VirtualBox.

I created the first virtual machine which I downloaded and installed which is called “Metasploit 2”. The configurations go as follows:

1. **Creation of VM1**

* I named the VM DC1.
* I allocated 80GB of disk space.
* I then assigned 1024 of RAM.

1. **The network configuration**:

* I configured the VM to use static IP address of 172.16.1.1
* Then I set the gateway to 172.16.1.100

1. **The installation of the Operating System**

* I booted the VM with the installation of the ISO and followed the

on- screen instructions to install the Operating System.

1. **Creation of VM2:**

* I named the VM Kali.
* I allocated 80GB of disk space.
* I then assigned 1024 of RAM.

1. **The network configuration:**

* I configured the VM to use static IP address of 172.16.1.2
* Then I set the gateway to 172.16.1.100

1. **The installation of the Operating System**

* I booted the VM with the installation of the ISO and followed the

on- screen instructions to install the Operating System.

* + I then set the hostname to Kali

1. **The configuration of the host machine**
   * I created a windows 10 host machine and manually set the static IP address to 172.16.1.3.
2. After completing the installation process, I then ensured that all machines (host and VMs) are on the same network segment. I verified the connectivity by pinging each of the machines from one another.
   * From VM1 (DC1) I pinged VM2 (Kali)
   * From VM2 (Kali) I pinged VM1 (DC1)

1.2)

A)

I opened the terminal window in the Kali Linux machine and used the IP command to list all network interfaces and their IP configurations. The command I used was **“IP** **addr show.”** Then I had to check the default gateway and to display the gateway I used the IP route command which is **“IP route.”**

B)

To scan the IP subnet on the network and to confirm the number of hosts and open ports to be discovered, to do so I had to use tools like nmap on the Kali Linux machine. The command that I used is **“sudo nmap –sP 172.16.1.0/24.”**

C)

When performing a banner grab, this is a method to gather information about network services running on open ports, these ports can help identify potentially vulnerable machines.

To scan for open ports and grab banners I used the nmap with the –sV flag to scan for open ports. The command used is **“sudo nmap –sV 172.16.1.0/24.”**

1.3)

1. **Social Engineering**: This is when exploiting human psychology to manipulate individuals into divulging confidential information or performing actions that compromise security, such as phishing attacks.
2. **Vulnerabilities in Software:** This comes when exploiting flaws or weaknesses in the software, such as unpatched software vulnerabilities, to gain unauthorized access to systems or data.
3. **Weak Authentication:** This is when taking advantage of weak or easily guessable passwords, the lack of multi-factor authentication or poor credential management or gain unauthorized access to accounts and systems.

**Question 2:**

**Conducting a Vulnerability Assessment for New Web Application:**

Ensuring the security of the web application is paramount, especially when handling sensitive customer data like the one of. In conducting a comprehensive vulnerability assessment this is crucial to identify and mitigate potential security risks. I will outline systematic steps, tools, and prioritization strategies involved in conducting such an assessment.

1. **Preparation and Information Gathering:**

*Step:*

* + **Is to Define the Scope:** This is to determine the boundaries of the assessment, including all features of the web application and any of the associated infrastructure.
  + **Is to Understand the Application:** To gather documentation, understanding the architecture, the data flow, and technologies used (e.g., the languages, frameworks, and databases).

*The Techniques and Tools:*

* + **The interviews and Questionnaires:** This is to talk to developers, administrators, and stakeholders.
  + **Documentation Reviews:** To analyze design documents, with the flow diagram, and architecture documents.
  + **The Automated Tools:** These use tools like Nmap for networking scanning and wappalyzer to identify technologies used.

1. **Threat Modeling:**

*Step:*

* + **To Identify Assets:** To determine the key assets such as customer data, user credentials, and transaction records.
  + **To Identify Threats:** To Use threat modeling frameworks to identify potential threats but I would also consider STRIDE which is (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

*The Techniques and Tools:*

* + **Microsoft Threat Modeling Tool:** Maps out the threat against identified assets.
  + **The OWASP Threat Dragon:** The open-source threat modeling tool for web applications.

1. **Automated Scanning:**

*Steps:*

* + **Static Analysis:** To review the application’s source code for vulnerabilities.
  + **Dynamic Analysis:** Tests the running application for vulnerabilities in real-time.

*The Techniques and Tools:*

* + **Static Application Security Testing (SAST):** The use of tools like **SonarQube** or **Fortify**
  + **Dynamic Application Security Testing (DAST):** To employ tools like **OWASP ZAP** or **Burp Suite** to scan the application.

1. **Manual Testing:**

*Step:*

* + **To Exploit Vulnerabilities:** A manual attempt to exploit vulnerabilities found during automated scanning.
  + **Penetration Testing:** Is a simulation that attacks to identify weaknesses not detected by automated tools.

*The Techniques and Tools:*

* + **OWASP Testing Guide:** Need to follow the OWASP testing guide for a structured approach.
  + **Burp Suite Pro:** This is for in-depth manual testing, including intercepting and modifying traffic.
  + **Kali Linux:** The use of various tools that are included in this distribution for manual testing (e.g., SQLMAP, Hydra).

1. **Analysis and Reporting:**

*Steps:*

* + **Risk Assessment:** To evaluate the impact and likelihood of each identified vulnerability.
  + **Prioritize Vulnerabilities;** To use a risk matrix or scoring system like CVSS (Common Vulnerability Scoring System).

*The Techniques and Tools:*

* + **CVSS Calculator:** Used to quantify the severity of vulnerabilities.
  + **Risk Matrix:** Maps the vulnerabilities on a matrix to visualize and prioritize based on impact.

1. **Remediation and RE-Testing:**

*Steps:*

* + **Recommended Fixes:** To provide detailed remediation advice for each identified vulnerability.
  + **Verify Fixes;** Re-test the application after fixes is applied to ensure vulnerabilities are resolved.

*The Techniques and Tools:*

* + **JIRA or Bugzilla:** To track remediation efforts and verify fixes.
  + **Re-Scanning:** Is the use of the same tools (SAST, and DAST) to confirm the vulnerabilities have indeed been fixed.